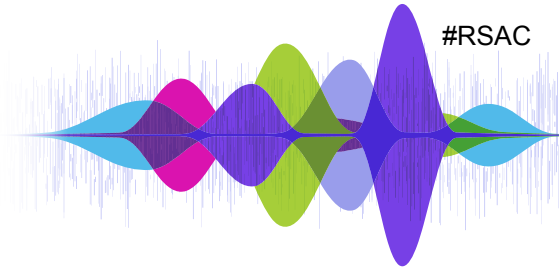
RSAC | 2025 Conference

Many Voices.
One Community.

SESSION ID: CLS-M05

So You've Deployed Kubernetes Everywhere, Now What?

Rory McCune
Senior Security Researcher & Advocate
Datadog
https://www.linkedin.com/in/rorym/

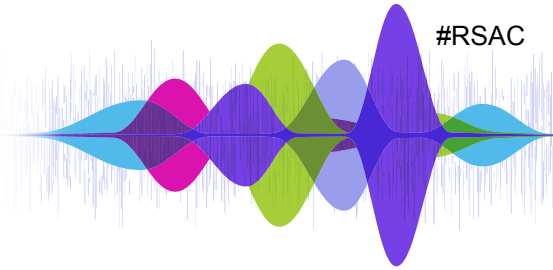


Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

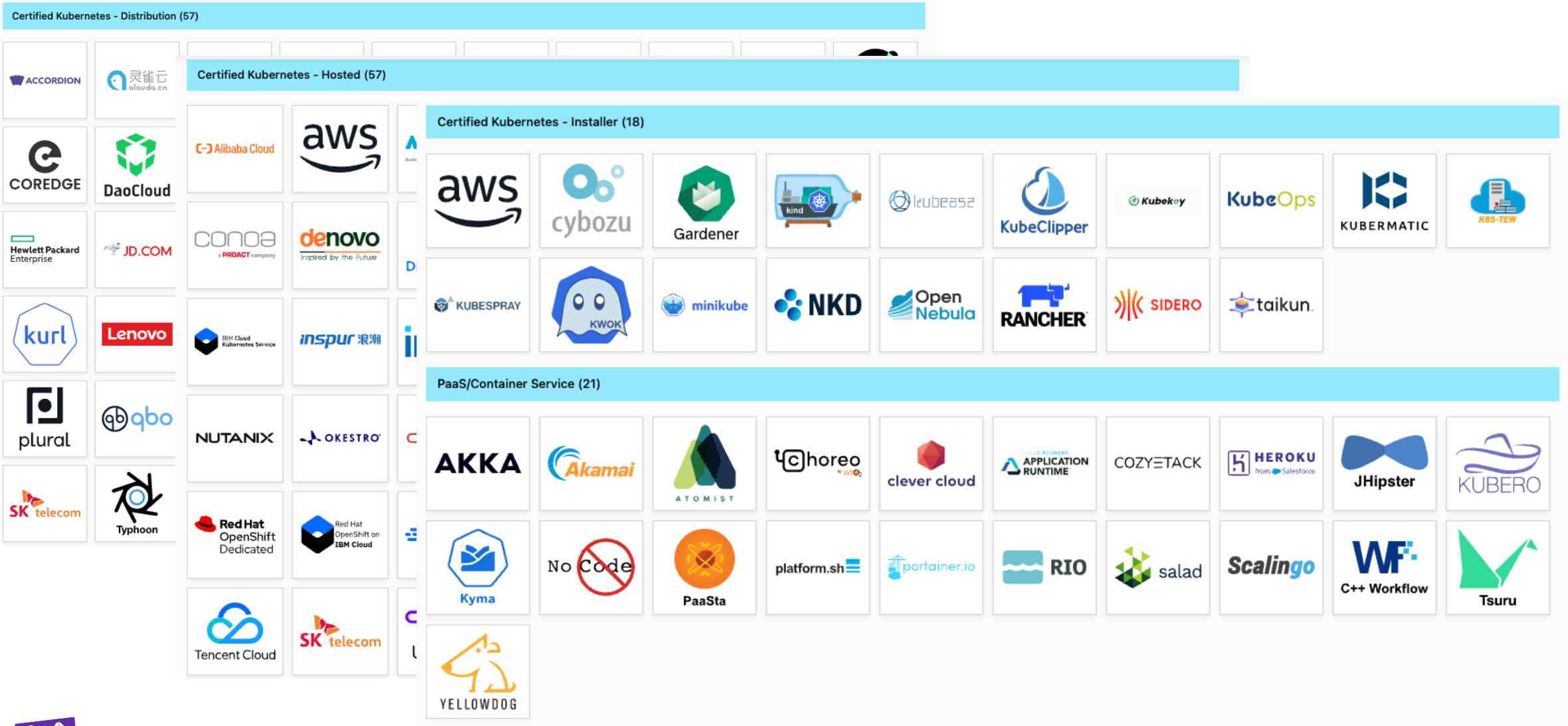


Introduction & Whom

- Senior security researcher and advocate at Datadog
- ~25 years in Information/IT/Cyber security
- Focusing on container security for ~9 years
- Maintainer of CIS Benchmarks for Docker and Kubernetes
- Work in the Kubernetes project including SIG-Security

Basic
Concepts

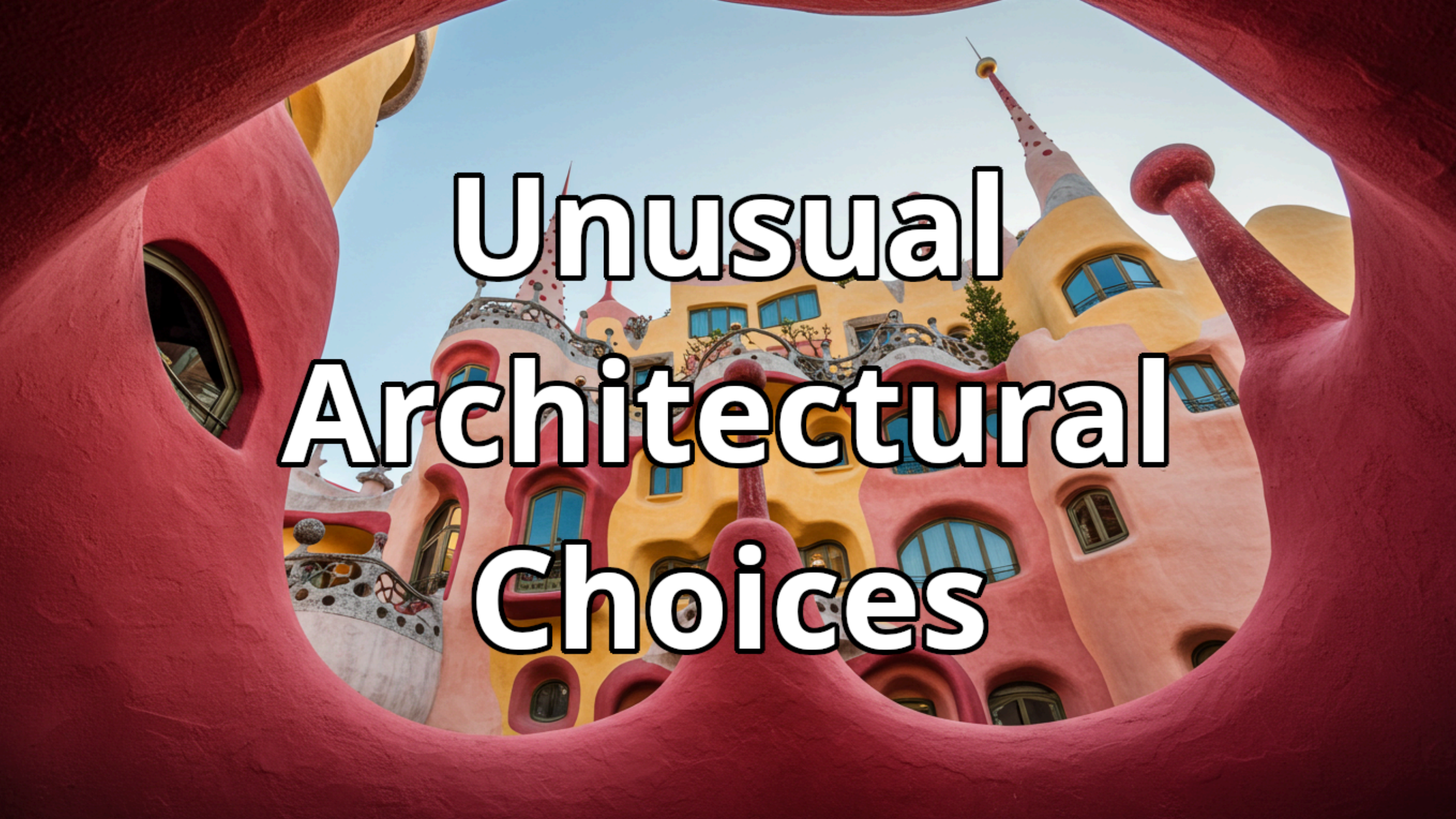
Distribution Variance



Managed
Kubernetes

Unmanaged
Kubernetes

Plugins


Unusual
Architectural
Choices

Flexible Authentication

- Kubernetes clusters can have one or more authentication providers
- Users can authenticate with any of them
- Most (production) clusters will use an external authentication source
- However internal sources are still present

No User Database

- Kubernetes does not have a user database!
  - Need to audit external authentication providers to know who has creds
- But, we have internal authentication mechanisms
  - For client certificates there is no persistent record of issued credentials or valid users
  - For service account tokens, there's a record of what valid accounts are but not issued credentials

Irrevocable Credentials

- Client certificates & service account tokens cannot be directly revoked
  - Rotate the CA key for the whole cluster for client certs
  - Delete the bound object for service accounts
- Credentials can have long lifetimes
- It’s possible to create new credentials for system accounts

Attack of the Clones

- With privileged access it's easy to clone system accounts using client certs or service accounts
- Provides hard to detect back door access to clusters
- Credentials often valid for years

File Edit View Bookmarks Plugins Settings Help

() neul × () neul × manifests : bash ×

```
rorym in 🌐 neul in  ⛵ gke_secure-moment-158819_us-central1-a_test-cluster ( ) ~/temp
❯
```

File Edit View Bookmarks Plugins Settings Help

() neul × () neul ×

```
rorym in 🌐 neul in  ⛵ myAKSCluster ( ) ~/temp
❯
```

Flexible Authorisation

- Similar to authentication, authorisation is flexible
- In practice rights will be the union of all authorisers
- Managed clusters will generally have 2+ authorisers.

RBAC is just String Matching

- Whilst most people think of the Kubernetes API as being CRUD
- Any other verbs can exist
- RBAC works by matching strings
- No registry of objects & verbs

Auditing Access

- A combination of these two issues makes it hard to audit rights to clusters
- Many Kubernetes tools only cover RBAC
- Few (no?) tools can create a unified view of effective rights

File Edit View Bookmarks Plugins Settings Help

() neul × () neul ×

```
rorym in 🌐 neul in  ⛵ gke_secure-moment-158819_us-central1-a_test-cluster ( ) ~/temp
❯
```

Create Pod == Root on Nodes by Default

- Kubernetes is distributed remote command execution as a service
- Without additional restrictions this means users who can create workloads can be root on the host
- Standard functionality, no hacks needed!

File Edit View Bookmarks Plugins Settings Help

() neul × () neul × manifests : bash ×

```
rorym in 🌐 neul in  ⛵ gke_secure-moment-158819_us-central1-a_test-cluster ( ) ~/temp
❯
```

Kubernetes API Server is a Proxy Server

- This is intended functionality
  - Allows for access to nodes and workloads without additional tools
- Essentially “SSRF as a service” for users with the correct rights
  - Restrictions on target address can be bypassed by known techniques
- Important to consider your threat model here

Security
Sharp Edges

System:masters Bypasses All Authorisation Checks

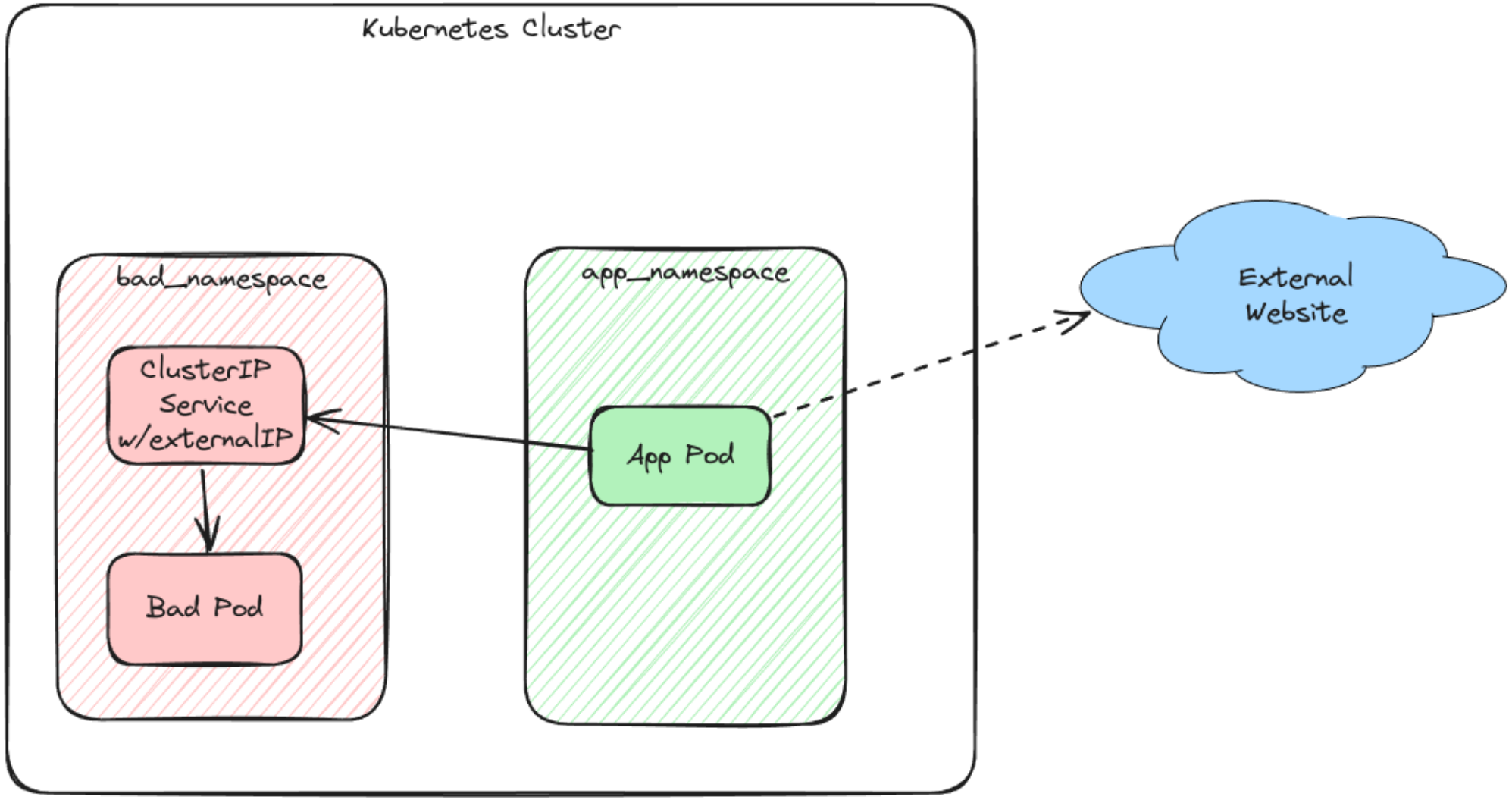
- system:masters is a group name hardcoded into Kubernetes
- Bypasses ALL authorisation checks
- Requests are not even sent to external authorisers
- Commonly used in initial accounts when clusters are setup

Kubelet API Bypasses Audit + Admission Control

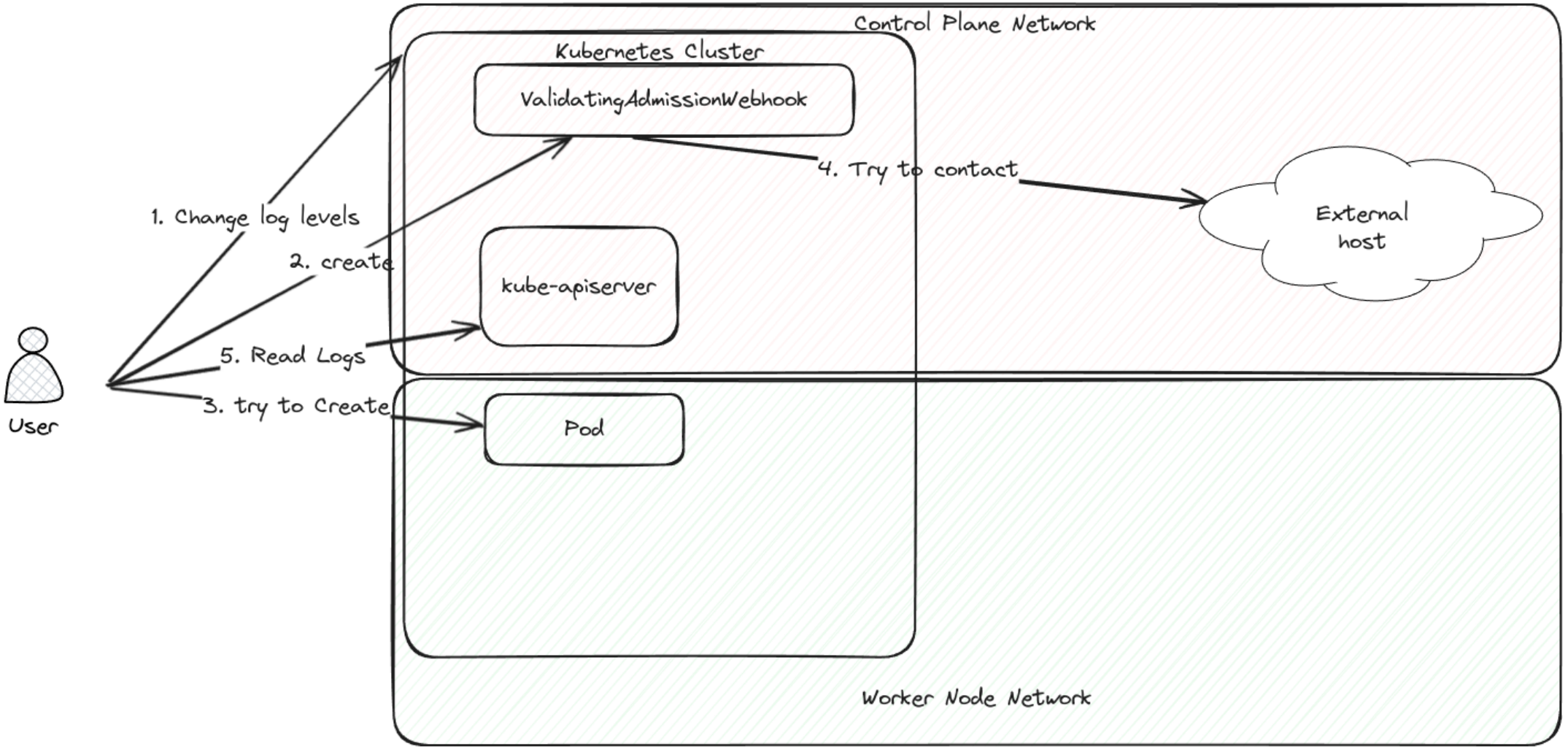
- The Kubelet (node agent) has its own API on 10250/TCP
- Supports command execution in every container on a host (amongst other things)
- No audit logging
- No admission control
- Access governed by Kubernetes RBAC (node/proxy)
  - Cluster privileged users automatically get access

The
Unpatchable
Four

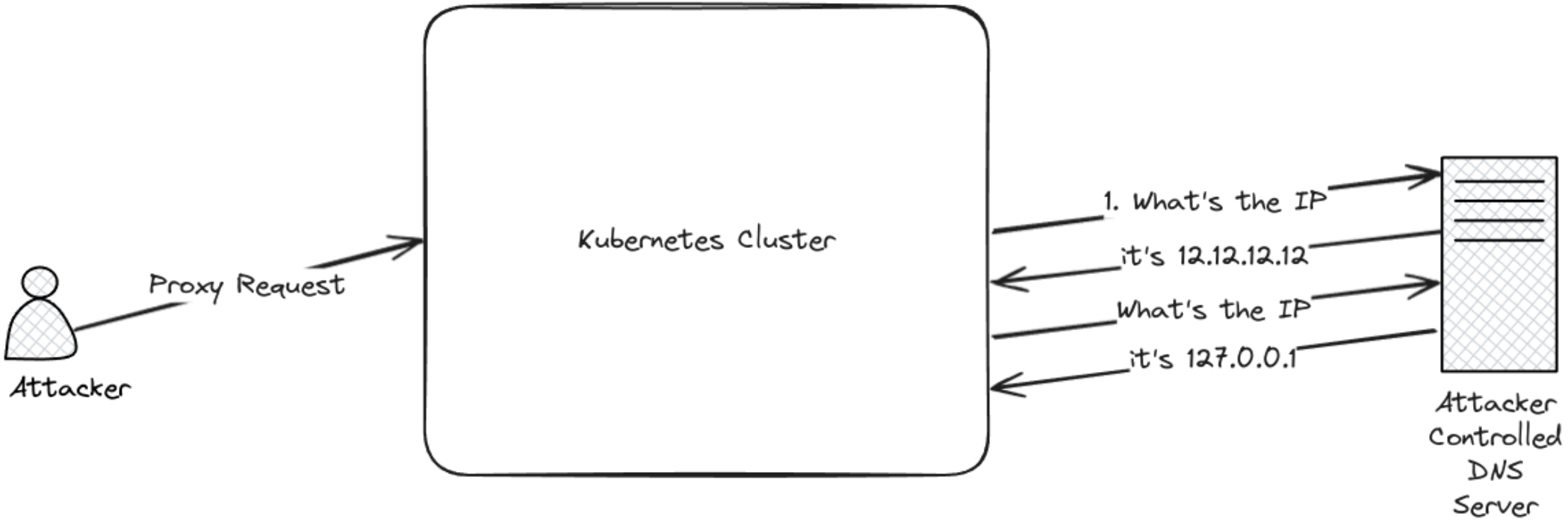
CVE-2020-8554



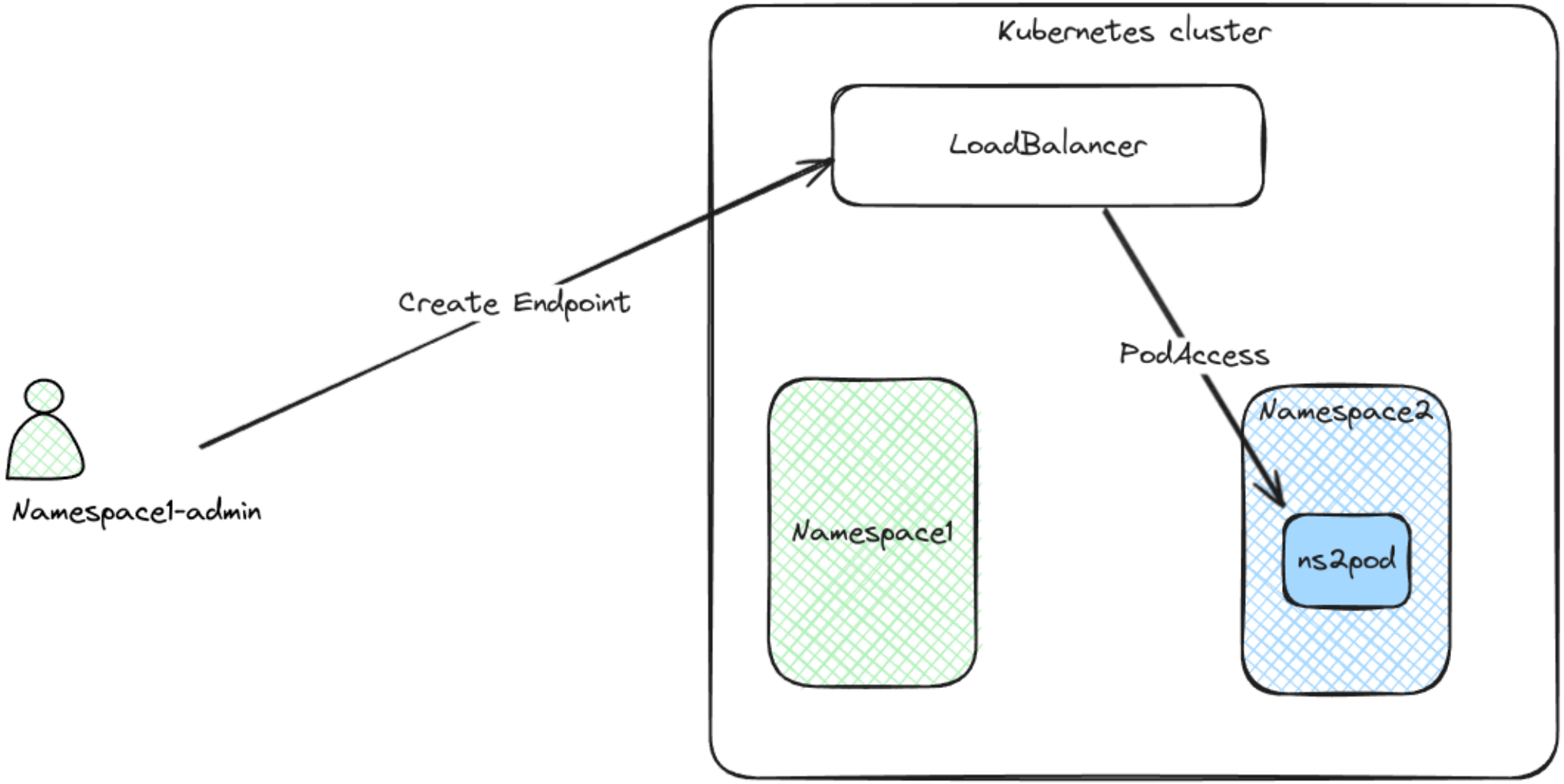
CVE-2020-8561



CVE-2020-8562

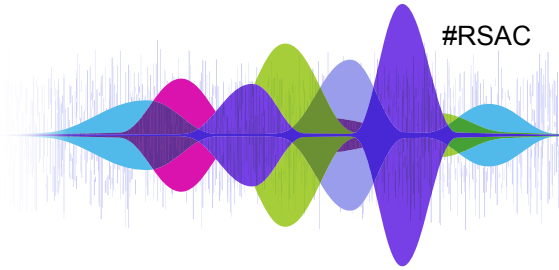


CVE-2021-25740



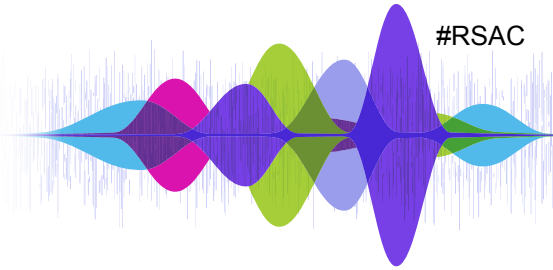
A Small Selection of Cloud Provider Defaults

- Internet accessible by default
- GKE Read-only Kubelet
- GKE system:authenticated is *everyone*
- AKS initial system:masters credential
- EKS Kube-proxy bound to all interfaces



“Apply” Slide

- Limit cluster exposure
- Enable Kubernetes audit logging
- Understand your cluster threat model
- Ensure appropriate visibility of AuthN and AuthZ configurations
- Ensure admission control restrictions are place for all users
- Have alerting in place for key attacks



Summary

- Kubernetes security can be a bit … complex
- It’s important to understand its architecture and how it fits in with your threat model
- There are quite a few security sharp corners to be aware of

Resources

- Datadog Security Labs - https://securitylabs.datadoghq.com/
- Security Labs Youtube - https://www.youtube.com/watch?v=jTswj4CS4IA&list=PLdh-RwQzDsaNWBex2I09OFLCph7I_KnQE
- Personal blog - https://raesene.github.io/

RSAC 2025 Conference

Many Voices.
One Community.

E-Mail: rory.mccune@datadoghq.com

Social media: @raesene@infosec.exchange